PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-296978
(43)Date of publication of application : 29.10.1999

(51)Int.Cl. G11B 20/10
G09C 5/00
G11B 20/12

(21)Application number : 10-093276 (71)Applicant : CANON INC
(22)Date of filing : 06.04.1998 (72)Inventor : TANAKA HIROKAZU

(54) INFORMATION RECORDING AND REPRODUCING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To more improve security by producing a ciphering key/a decoding key based on the data recorded in a sector front by a prescribed number from a sector in which a recording/a reprodution is to be performed for every sector in order to ciphering/decoding data based on the data already recorded on a record medium.
SOLUTION: An MPU 33 reproduces the data recorded in a sector which is preceding the sector going to record to produce a ciphering key based on the read data. When the ciphering key is produceddata which are transmitted from a host computer 32 are ciphered together with a recording command by the obtained ciphering key in a ciphering/decoding circuit 42 and the ciphered data are recorded from the recording starting position of a block which is selected at present. The above-mentioned processings are repeatedly performed for every sector in which a reproding is to be performed and a ciphering key is produced based on the data of a sector ahead by one sector for every sector and data are ciphered by using this key and the ciphered data are recorded on the record medium.

CLAIMS

[Claim(s)]
[Claim 1]A means which records / reproduces data at an added type recording medium of a postscript which has two or more tracks which comprise one or more

sectorsIn the Information Storage Division playback equipment which has a means which records / reproduces a directory for managing data to said recording mediuma means to encipher data before record of dataand a means to decrypt reproduced dataIt has a means to create the cryptographic key / decryption key for enciphering / decrypting data based on data already recorded on said recording mediumInformation Storage Division playback equipmentwherein said cryptographic key / decryption key preparing means create a cryptographic key / decryption key based on data in which only a predetermined number is recorded on a front sector for every sector after this from record / sector to reproduce.
[Claim 2]The Information Storage Division playback equipment according to claim 1 when said cryptographic key / decryption key preparing means is not recorded [data] on a front sector only said predetermined numberwherein it creates a cryptographic key / decryption key based on a default value decided beforehand.
[Claim 3]The Information Storage Division playback equipment according to claim 1 recording said predetermined number on said directory.
[Claim 4]The Information Storage Division playback equipment according to claim 3 changing a predetermined number recorded on said directory for every file of said recording medium.
[Claim 5]The Information Storage Division playback equipment according to claim 1wherein said recording medium is an optical card.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to an information recording medium about the Information Storage Division playback equipment which records / reproduces information especially at a data encryption/decryption.
[0002]
[Description of the Prior Art]Various kinds of thingssuch as the shape of a diskcard shapeand tape shapeare known as a gestalt of the medium which records information optically conventionally or reads the recorded information. The optical information recording medium (an optical card is called below) formed in card shape among these mediaAlthough it has one thousands times - 10000 times the storage capacity of this as compared with a magnetic card and rewriting is impossible like an optical discsince the storage capacity is as large as 1-6 M bytesthe application range wide as a prepaid card etc. which are used for the passbook of a banka portable mapor shopping is considered.

[0003]When recording data on such an optical card and reproducing to itit is common to usually record the directory for managing data with data on some optical cardsand to manage data for every file. The directory comprises information required for file managementsuch as a file namea start address of initial dataand a sector number recorded continuouslyas shown in drawing 3. Whenever this directory records datait is recorded on a part of record section of an optical card as management information of data.
[0004]Drawing 4 is an outline top view of an optical card1 is an optical card and 2 is the Information Storage Division field. In the Information Storage Division field 231-3n of tracking track+1 places a constant intervalit is arranged in paralleland 41-4 n of code tracks for recording information between each of that tracking track are formed. 51-5 n of physical track numbers for identifying a code track are beforehand added to the both ends of each code track. In the optical card of drawing 4the Information Storage Division field 2 is divided into two blocks in the code track 42 - 4k by considering the block 61 and code track 4k+1-4n-1 as the block 62. Dividing the optical card 1 into two or more blocks is indicated to JPS63-244385A.
[0005]For exampleit is possible to record electrocardiogram information on the block 61 and it to record blood-pressure information on the block 62when recording a patient's electrocardiogram information and blood-pressure information in thisusing an optical card as a medium for medical information record. It is the block 61when a block division is performed for every kind of data recorded in this way and electrocardiogram information is reproduced. Access time can be shortened in order for what is necessary to be to reproduce only inner data. Of coursethe number of partitions of a block and the number of code tracks within a block can be arbitrarily set up according to the kind and data volume of data to record.
[0006]In the optical card 1the method which changes one the sector number and sector size of a code track for every block is known. Drawing 5 shows the example of the sector size of dataand the relation of a sector number recorded on one code track. In drawing 5the sector type 1 records 1024 bytes of sector on the one code track 4The sector type 2 records 512 bytes of sector on the two code tracks 4The sector type 3 records 256 bytes of sector on the four code tracks 4It is shown that the sector type 4 records 128 bytes of sector on the six code tracks 4the sector type 5 records 64 bytes of sector on the eight code tracks 4and the sector type 6 records 32 bytes of sector on the 12 code tracks 4.
[0007]Although what is necessary is just to be such a methodand to record one sector (one code track) when recording 768 bytes of data by the sector type 1for exampleif it records by the sector type 624 sectors (two code tracks) must be recorded. Thereforewhen it records by the sector type 6it not only

takes timebut it will make storage capacity of an optical card useless. When recording 32 bytes of data by the sector type lone code track will be usedbut if it records by the sector type 6it will end with one sector and only 1/12 of code tracks will be used compared with the sector type 1. An access speed is not only made earlybut by choosing a sector type according to the data size recorded in this wayit can use the record section of an optical card effectively.

[0008]The data in which 711-71i are recorded in the block 61 in drawing 4 hereand 7 21.-72j are data currently recorded in the block 62. They are a directory for 811.-81i to manage the data 71 currently recorded in the block 61and a directory for 821.-82j to manage the data 72 currently recorded in the block 62. Data is added in the direction of B and the directory is added in the direction of F. The data 71 and its management information are recorded for electrocardiogram informationand it should just record 72 and its management information for the directory 81 and blood-pressure information as 82when recording medical information on an optical card as mentioned above.

[0009]When recording the information that data volume is biglike electrocardiogram informationa sector size is enlarged like the data 711-71iand an access speed can be brought forward if the sector number recorded on one code track is set to one. On the contrarylike blood-pressure informationwhen data volume is smalla sector size is made small like the data 721-72jand if the sector number recorded on one code track is increasedthe storage capacity of an optical card can be used effectively. Since the data size of a directory is comparatively smallit is good to recordfor example by the sector type 5.

[0010]In the code track 41 and the code track 4n belonging to neither of an optical card of the blocks. The optical card management information 9 (format information is called hereafter)such as the block number of partitions of the optical card 1 mentioned abovea track number of each blockand a sector type used with each blockis recorded. Drawing 6 is a figure showing the contents of this format informationand it is the information which shows that top identification information is format informationfor examplethe information of "FMT" is recorded by an ASCII code. The following block number of partitions is information which shows into how many blocks the optical card 1 is divided. Nextthe information which shows each number of code tracks and sector type of the block 61 - the block 6n is recorded.

[0011]By the wayrecord and reproduction of the information on an optical card can be carried out by arbitrary users. Thereforewhen many users use itrequired information may be destroyed accidentallyinformation may be altered intentionallyor others may look at the high information on confidentiality. Theninformation (password information is called below) peculiar to an

individual is recorded for every block of an optical cardWhen recording or reproducing data in the block with which password information is recordedPassword information is inputtedthe inputted password information and the password information currently recorded in the block are comparedand only when a collated result is in agreementthe method of permitting the record reproduction of the information within a block is adopted.
[0012]1011 and 1012 of drawing 4 are the password information of the block 61. This password information comprises identification information and password informationas shown in drawing 7. It is the information which shows that identification information is password informationand the information of "PWD" is used by an ASCII codefor example. Nextactual password information is recorded. When carrying out record reproduction of the electrocardiogram information by using such password informationfor examplepassword information is inputted from a host computerand only when this is in agreement with the password information within the block 61access of electrocardiogram information is attained. On the other handsince password information is not recorded on track 4k+1 which records the password within the block 62and 4n-1the record reproduction of blood-pressure information is freely possible.
[0013]Howeverby modulating the optical beam extracted in the shape of fine spot according to recorded informationand scanning the modulated optical beam on a code trackwhen recording information on an optical cardSince it records as a detectable pit sequence opticallyeven if a password restricts access within the block 6if analyzed using an optical microscope etc. the high information on confidentiality may be seen by others. Thenin order to raise securityit enciphers by a cryptographic keythe data recorded on an optical card is recordedand the method of decrypting the enciphered data by a decryption key at the time of reproductionand reproducing is proposed.
[0014]The data which analyzed the data recorded on the optical card by using this method even when analyzed by an optical microscope etc. becomes what does not make a meaningand the confidentiality of the data recorded on the optical card can be maintained. Various methods can be considered as a method which enciphers the data recorded on an optical cardand although the RSA cryptograph of a public key systemthe DES code of a common key systemetc. are famousin order to explain simplythe Cesar code is explained to an example here. When the number which expresses c and a cryptographic key with the Cesar code for the number which expresses [a number] one character of x and a cryptogram for A= 0B= 1--the number with which it is made to correspond with Z= 25 and one character of a plaintext is expressed to the alphabet is set with kit is a cipher system expressed with the expression of relations of c=(x+k) mod 26. Howevera mod n shows the remainder which broke a by n. In the decryption which makes a cryptogram a plaintextit is expressed with the expression of relations

of x=(c-k) mod 26. Thereforein the Cesar codea cryptographic key and a decryption key turn into the same key. And when cryptographic key k is 1for exampleif a plaintext is "ABC"a cryptogram will be enciphered as "BCD." Howeversince only the character of the alphabet can be treated the way things standIt becomes possible by extending the formula of encryption like c=(x+k) mod 256and extending the formula of decryption like x=(c-k) mod 256 to treat all the characters expressed with 1 byte. And since performing at high speed is desirable as for these encryption or decryptionit is common to carry out by hardware.

[0015]Nextthe preparation method of a cryptographic key is explained. Although the preparation method of a cryptographic key can consider various methodsa cryptographic key can be created by inputting into a certain function the information on format informationpassword informationa directoryetc. which are recordedfor example on the optical card. Thereforeit is k=F (n) when the password for creating k and a key for a cryptographic key is set to n. ******** is realized. Howeverthe function F (n) is a function which creates a cryptographic keyand a compressibility function etc. are used. A compressibility function is a function which changes the bit string of arbitrary bit length into the bit string of a certain length. Optical card Information Storage Division playback equipment performs a data encryption and decryption of the enciphered data using this cryptographic key.

[0016]Nextthe optical card Information Storage Division playback equipment which records or reproduces information to an optical card is explained. Drawing 8 is a block diagram showing the outline composition of optical card Information Storage Division playback equipment. In drawing 831 is optical card Information Storage Division playback equipment which records information on the optical card 1 and is reproduced to itand is connected to the host computer 32 of an upper control apparatus. Information Storage Division playback equipment 31 performs record of informationand reproduction based on control of the host computer 32. 37 is a card feed motor for driving an unillustrated conveyer styleand introducing the optical card 1 into the prescribed position in Information Storage Division playback equipment 31carrying out reciprocation moving of the optical card 1 in the direction of R in a prescribed positionand also discharging the optical card 1 outside the plane. 38 is an optical beam irradiation optical system containing the semiconductor laser of a light sourceextracts the optical beam of a light source to minute light spot at the time of record of informationand reproductionand irradiates with it on the optical card 1.

[0017]The photodetector with which 39 detects the light reflected from the optical card 1and 40 drive a part of optical beam irradiation optical system 38and the focus position of the light spot on the 1st page of an optical card

A Z directionNamelyAF actuator for making it move to an optical card side and a perpendicular directionand performing autofocus control41 is AT actuator for driving a part of optical beam irradiation optical system 38moving the light spot on the 1st page of an optical card in the direction of Yi.e.the direction which intersects perpendicularly with the code track of an optical cardand performing auto tracking control. The optical head 30 is constituted including these optical beam irradiation optical systems 38the photodetector 39the AF actuator 40and the AT actuator 41. 36 is a head feed motor for moving the optical head 50 in the direction of Yand accessing light spot on a desired track.

[0018]MPU33 is a processor circuit for controlling each part in Information Storage Division playback equipment 31and builds in ROM and RAM. MPU33 controls the head feed motor 36the card feed motor 37etc.and performs transmission and reception of the host computer 32 and data. The AT/AF control circuit 34 detects an AT/AF control signal from the output signal from the photodetector 39Based on itthe AF actuator 40 and the AT actuator 41 are drivenand autofocus control and auto tracking control are performed so that the light spot from the optical beam irradiation optical system 38 may connect a focus to a card surfaceand light spot may follow and scan to a code track.

[0019]The modulation and demodulation circuit 35 is a circuit for modulating record data based on control of MPU33and the circuit for restoring to regenerative dataand the encryption/decoding circuit 42 enciphering record dataand decrypting regenerative data. At the time of record of informationrecord data is transmitted to MPU33 from the host computer 32and record data is enciphered after that in encryption / decoding circuit 42. In the modulation and demodulation circuit 35the enciphered data is modulatedthe light source within the optical beam irradiation optical system 38 is driven according to a modulating signaland information is recorded by scanning the optical beam of this modulated light source to the code track of the optical card 1.

[0020]On the other handat the time of reproduction of informationthe optical beam for reproduction is scanned from the optical beam irradiation optical system 38 to the code track of the optical card 1and the photodetector 39 detects the catoptric light from the optical card 1. At this timethe modulation and demodulation circuit 35 generates an information reproduction signal from the output signal of the photodetector 39and restores to a regenerative signal. The data to which it restored is stored in RAM of MPU33and the data enciphered by encryption / decoding circuit 42 is decrypted after that. The decrypted data is transmitted to the host computer 32 from MPU33. The host computer 32 performs transmission and reception of Information Storage Division playback equipment 31and a command and dataand performs

record and reproduction of information for every sector.
[0021]Nextthe operation at the time of accessing the data of an optical card in optical card Information Storage Division playback equipment is explained with reference to drawing 9. In drawing 9Information Storage Division playback equipment 31 is supervising first whether the optical card 1 was inserted (S901). Insertion of an optical card will reproduce the format information 9 first (S902). When format information is reproducedit understands how the record section of the optical card 1 is divided. In this casebased on format informationthe block 61 is automatically chosen as a default blockand the password information 101 of the block 61 is reproduced (S903). Password information is memorized to RAM in MPU33and if the password is not recordedit will memorize to RAM that this block is not protected by a password.
[0022]Subsequentlythe directory 81 of the block 61 is reproduced one by oneand it memorizes in the order read into RAM in MPU33 (S904). Since data and a directory are sequentially recorded on the optical card 1if a directory is reproducedthe recording start position of a directory and the recording start position of data can be found from the number of the reproduced directoriesand the contents of the reproduced directory. Thusthe optical card Information Storage Division playback equipment 31 will be in the state of waiting for the command from the host computer 32 (S905)and will perform the following processings according to the kind of command. Firstit is confirmed whether a command is a discharge command (S906). When a command is a discharge commanddischarge of the optical card 1 is performed and the processing to this optical card 1 is ended (S907).
[0023]On the other handit confirms whether be a password examination commandwhen a command is not a discharge command (S908)and a password is compared when it is a password examination command (S909). That isthe password which was reproduced by S903 and memorized to RAMand the password sent from the host computer 32 by the password examination command are compared. Herewhen both passwords are in agreementit memorizes that the password in the block 61 is ending with collation to RAM in MPU33. When a password is not in agreementit shifts to the waiting processing for a command of S905 as it is. When the block chosen now is not protected by a passwordcollation is not performed but it returns to S905.
[0024]After ending the collation processing of a passwordit confirms whether a command is a block select command (S910)and when it is a block select commandthe password information of the block specified based on the format information reproduced by S902 is reproduced (S911). The reproduced password information is memorized to RAM in MPU like S903. Subsequentlyall the directories currently recorded on the specified block are reproduced (S912)it memorizes in the order read into RAM in MPU33and processing of block selection

is ended.
[0025]On the other handwhen a command is not a block select command in S910a command is a record command or a reproduction command.
Since a password must confirm [ending with collationor] when the block chosen now is protected by the passwordorwhen being investigated and (S913) protectedand when [that are protected by the password]it confirms first whether to be finishing [a password / collation] (S914).
This check is performed by referring to the information memorized to RAM by S909. When a password is not ending with collationit returns to S905. When a password is ending with collationand when it is judged that it is not protected by a password in S913it shifts to the following processing of S915.
[0026]In S915it confirms whether a command is a record commandand when it is a record commanda cryptographic key required for encryption is created (S916). A cryptographic key is created based on the directory of the last memorized by RAM. This directory is a directory recorded on the block accessed now at the end. When it is the first data to record on this blocksince the directory is not recorded on this blocka cryptographic key is still created based on the default value decided beforehand. The above compressibility functions are used for creation of a cryptographic key.
[0027]Subsequentlyit records from the position which should start record of the block which enciphers the data sent from the host computer 32 with the record command by the cryptographic key created from the directory by S916 (S917)and is chosen in the enciphered data now (S918). Thenthe directory for managing the recorded data is recordedthe same directory also as RAM is memorized (S919)and processing of a record command is ended.
[0028]On the other handwhen it is not a record command in S915it is confirmed whether a command is a reproduction command (S920). Since it is a command which Information Storage Division playback equipment 31 does not support when it is not a reproduction commandit returns to S905and a decryption key is created when it is a reproduction command (S921). A decryption key searchs the directory of the data which should be reproduced from the directory memorized by RAMand creates it based on the directory in front of [of the directory] one. When there is no directory in front of onea decryption key is created based on the default value decided beforehand. Subsequentlyit asks for the sector dress which should be reproduced from the file name specified by the record commandand the directory memorized to RAMand data is reproduced (S922). Since the data reproduced here is the enciphered datait is decrypted using the created decryption key (S923)transmits the decrypted data to the host computer 32and ends regeneration.
[0029]
[Problem(s) to be Solved by the Invention]In the conventional methoda

cryptographic key is created from the directory of a file recorded at the endand the decryption key is created from the directory of the file before [of the file to reproduce] one. That issince it was enciphering/decrypting for every fileafter one key was specifiedthe whole file will be decoded and there was a problem that security was low.

[0030]In view of the above-mentioned conventional probleman object of this invention is to provide the Information Storage Division playback equipment which can be further improved in security by changing a cryptographic key / decryption key for every sector.

[0031]

[Means for Solving the Problem]A means which records / reproduces data at an added type recording medium of a postscript which has two or more tracks with which the purpose of this invention comprises one or more sectorsIn the Information Storage Division playback equipment which has a means which records / reproduces a directory for managing data to said recording mediuma means to encipher data before record of dataand a means to decrypt reproduced dataIt has a means to create the cryptographic key / decryption key for enciphering / decrypting data based on data already recorded on said recording mediumSaid cryptographic key / decryption key preparing means are attained by the Information Storage Division playback equipment creating a cryptographic key / decryption key based on data in which only a predetermined number is recorded on a front sector for every sector after this from record / sector to reproduce.

[0032]

[Embodiment of the Invention]Hereafteran embodiment of the invention is described in detail with reference to Drawings. Firsta 1st embodiment of this invention is described. Composition of the hardware of the Information Storage Division playback equipment by a 1st embodiment shall be considered as the same composition as drawing 8and shall use the optical card of drawing 4 as a recording medium. Drawing 3 and a sector type shall use drawing 5format information shall use drawing 6andas for the directory for managing the file data recorded on the optical card 1password information shall use the thing of drawing 7. Since these drawing 8drawing 4drawing 3drawing 5drawing 6and drawing 7 were described previouslydetailed explanation is omitted.

[0033]Drawing 1 is a flow chart which shows operation of this embodiment. Since it is the same as S901-S915 of drawing 9 in which the conventional operation is shownS101-S115 of drawing 1 are explained briefly. In drawing 9firstif the optical card 1 is inserted in Information Storage Division playback equipment 31 by S101the format information of the optical card 1 will be reproduced (S102). If format information is reproducedthe dividing state of a block of the optical card 1 is knownin this embodimentthe block 61 will be

automatically chosen as a default block as usualand the password information of the block 61 will be reproduced (S103). Password information is memorized to RAM in MPU33. When password information is not recordedit memorizes to RAM that this block is not protected by a password.
[0034]Subsequentlysince the directory 81 of the block 61 is reproduced one by one (S104)it memorizes in the order read into RAM in MPU33 and data and a directory are sequentially recorded on the optical cardThe recording start position of a directory and the recording start position of data are obtained from the number and contents of the reproduced directory. NextInformation Storage Division playback equipment 31 executes the command from the host computer 32 for the following processings according to the kind of waiting (S105) and command. Firstit confirms whether a command is a discharge command (S106)if a command is a discharge commandthe optical card 1 will be dischargedand the processing to this optical card is ended (S107). A password is compared when it is [whether when it is not a discharge commandit is a password examination commandand] a check (S108) and a password examination command (S109). That isif the password memorized to RAM and the password sent from the host computer 22 by the password examination command are compared and both passwords are in agreementit will memorize that the password in the block 61 is ending with collation to RAM in MPU33. When a password is not in agreementit shifts to the waiting processing for a command of S105.
[0035]On the other handwhen it is not a password examination command in S108it confirms whether to be a block select command (S110). If it is a block select commandthe password information of the block specified based on the format information reproduced by S102 will be reproduced (S111). Password information is similarly memorized to RAM. Subsequentlyall the specified directories of a block are reproduced (S112)it memorizes in the order similarly read into RAMand processing of block selection is ended. When it is not a block select command and the block which a command is a record command or a reproduction command and is chosen now is protected by the passwordSince a password must confirm [ending with collationor]orwhen being investigated and (S113) protectedand when [that are protected by the password]it confirms first whether to be finishing [a password / collation] (S114). This is performed by referring to the information memorized to RAM. When a password is not ending with collationit returns to S105and when a password is ending with collationand not protected by a password by S113it shifts to the following S115.
[0036]In S115it confirms whether a command is a record commandand when it is a record commanda cryptographic key required for encryption is created (S116). According to this embodimentonly a predetermined number makes the data of a front sector a password from the sector to be recorded from now onand a

cryptographic key is createdfor examplethe cryptographic key is created from the data of the sector in front of one here. Although what kind of thing it may be sufficient as the compressibility function for creating a cryptographic keylet the value of 1 byte which added all the bytes of the sector in front of one by exclusive OR be a cryptographic keyfor example. The cryptographic key is created by MPU33.

[0037]ThereforeMPU33 reproduces the data currently recorded on the sector in front of [of the sector to be recorded from now on] oneand creates a cryptographic key based on the data. This data is the data recorded on the block accessed now at the endand when recording data on this block for the first timesince data is not recorded on this blocka cryptographic key is still created based on the default value decided beforehand. Creation of a cryptographic key will encipher the data sent from the host computer 32 with the record command by the cryptographic key created in encryption / decoding circuit 42S116 (S117). Subsequentlythe enciphered data is recorded from the recording start position of the block chosen now (S118). Processing of S116 to S118 is recorded by enciphering using the cryptographic key to record and which carried out repeatedly for every sectorcreated the cryptographic key based on the data of the sector in front of one for every sectorand was created for every sector. Thenthe directory which manages the recorded data is recordedthe same directory also as RAM is memorizedand processing of a record command is ended (S119).

[0038]Nextwhen it is not a record command in S115since it is whether a command is a reproduction command and a command which are checked (S120)and Information Storage Division playback equipment 31 does not support when it is not a reproduction commandit returns to S105. A decryption key is created when it is a reproduction command (S121). The file name specified with the reproduction command in this embodiment when a decryption key was createdIt asks for the sector address which should be reproduced from the directory memorized to RAMand only the predetermined number of the sectors subsequently reproduced reproduces the data currently recorded on the front sectorand is creating the decryption key based on the data. A decryption key is created by MPU33 and is creating the decryption key here based on the data currently recorded on the sector in front of [of the sector reproducedfor example] one. When there is no sector in front of onea decryption key is created based on the default value decided beforehand.

[0039]Since the data which reproduced data (S122) and was reproduced here is the enciphered data when a decryption key is createdthe data which decrypted and decrypted data using the decryption key created by encryption / decoding circuit 42 is transmitted to the host computer 32 (S123). Processing of S121-S123 is repeatedly performed for every sector to reproducecreates a decryption

key based on the data of the sector in front of one for every sectorand reproduces data. If all the sectors directed from the host computer 32 are reproducedit will be in the state of returning to S105 again and waiting for a command.

[0040]Thussince record / the cryptographic key / decryption key of data to reproduce is created in this embodiment after this based on the data currently recorded on the sector in front of predetermined ****A cryptographic key can differ from a decryption key for every sectorand other sectors cannot be temporarily decoded as the cryptographic key / decryption key ********** of a certain sectorbut security can be substantially raised compared with the former. It is hard to notice that it is a password since the data for creating a cryptographic key and a decryption key is not what was recorded as a passwordand even if a record section is analyzedthere is an advantage which cannot specify a password easily.

[0041]Nexta 2nd embodiment of this invention is described. Although it is considering [of the sector which creates a cryptographic key and a decryption key and which is case / the sector /recorded or reproduced] as immobilization how many it creates based on the data of a front sector in a 1st embodimentit is changed for every file in this embodiment. The predetermined numerical value which specifically shows how many a cryptographic key and a decryption key are created for the data of a front sector in a directory using the directory of drawing 2 is recorded. When this predetermined value records data for every file with Information Storage Division playback equipment 31 or the host computer 32it shall choose and record any value.

[0042]Although operation of this embodiment is the same as that of drawing 1it was judged as the record command by S115 -- coming -- the directory already read into RAM. That iswith reference to the predetermined value contained to the directory of a file to recordonly a predetermined value creates a cryptographic key based on the data currently recorded on the front sector from the sector to record (S116). Subsequentlydata is enciphered using the created cryptographic key (S117)and it records on the optical card 1 (S118). Processing of S116-S117 is repeatedly performed for every sectorand from the sector recorded for every sectoronly a predetermined value creates a cryptographic key based on the data of a front sectorand records data. If all the sectors directed from the host computer 32 are recordedthe directory for managing record data will be recorded (S119)and recording processing will be ended. When beginning and recording a filea predetermined value is decided with Information Storage Division playback equipment 31 or the host computer 32a cryptographic key is created using the valueand when recording a directorythe directory containing a predetermined value is recorded.

[0043]The predetermined value contained to the directory (already read into

RAM) which has the file name specified from the host computer 32 on the other hand when it was judged as a reproduction command by S120 is referred toOnly a predetermined value creates a decryption key based on the data currently recorded on the front sector from the sector reproduced using the value (S121). Subsequentlydata is reproduced by S122 and data is decrypted using a decryption key by S123. Perform processing of S121-S123 repeatedly for every sectorand only a predetermined value creates a decryption key based on the data of a front sector for every sectorIf all the sectors which reproduce data and which were directed from the host computer 32 are reproducedit will be in the state of returning to S105 again and waiting for a command.

[0044]Since a predetermined value is recorded on a directory and the cryptographic key and the decryption key are created in this embodiment using the valueFrom the sector which records or reproduces a cryptographic key and a decryption keyit can be changed how many it creates based on the data of a front sector the whole fileand security can be further raised compared with a 1st embodiment.

[0045]In an above embodimentalthough the Cesar code is used as an encryption algorithmother encryption algorithmssuch as DESmay be used. Since especially DES is more complicated than the Cesar code and it is hard to decodesecurity can be raised more. As long as it is a recording medium of not only an optical card but the added type of a postscript as an information recording mediumwhat kind of medium may be used.

[0046]

[Effect of the Invention]As explained aboveaccording to this inventionwhen only a predetermined number creates encryption/decryption key based on the data of a front sector for every sector after this from record / sector to reproduceEven if data can be enciphered / decrypted using different cryptographic key / decryption key for every sector and the key of one sector is specifiedother sectors cannot be decoded but can improve security substantially compared with the former. It is hard to notice that it is a password since data is not what was recorded as a passwordSince it becomes difficult to specify a password and it is not necessary to record a password on a data area apart from data even if a record section is analyzedthe part record section can be used effectively. Security can be further improved by recording a predetermined number on a directory and changing the value for every file.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a flow chart which shows operation of a 1st embodiment of the Information Storage Division playback equipment by this invention.
[Drawing 2]It is a figure showing the directory used for a 2nd embodiment of this invention.
[Drawing 3]It is a figure showing the directory of a conventional example.
[Drawing 4]It is a figure showing the example of an optical card.
[Drawing 5]It is a figure showing a sector type example.
[Drawing 6]It is a figure showing the example of FO mad information.
[Drawing 7]It is a figure showing the example of password information.
[Drawing 8]It is a figure showing the example of optical card Information Storage Division playback equipment.
[Drawing 9]It is a flow chart which shows the operation which accesses the optical card of the device of drawing 8.
[Description of Notations]
1 Optical card
2 Record section
4 Code track
6 Block
7 Data
8 Directory
9 Format information
10 Password
31 Optical card Information Storage Division playback equipment
32 Host computer
33 MPU
34 AT/AF control circuit
38 Optical beam irradiation optical system
42 Encryption/decoding circuit